Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Encryption Key Security**		Date Created:		**02-15-18**	
Standard Policy #	**2.12.3**	**Section** Title**:**	**Management of System**		Status	**Draft**
Approval Authority:	**ISICSB**		Adopted:		Reviewed:	

1. Purpose or Objective

The purpose of this standard is to establish policy and procedures for the security of encryption keys and the proper method of generating encryption keys used on the ISICS radio system network. This standard outlines the minimum steps that should be taken to secure any encryption key on the ISICS Platform.

2. Technical Background

- **Capabilities**

Encryption keys are used in end user equipment where encrypted voice communications are utilized. This includes, but may not be limited to, subscriber radios, dispatch consoles and radio voice logging equipment. Encryption keys are typically stored in Key Fill Devices (KFD), Key Management Facilities (KMF) or locked in a secure facility with limited access. Encryption utilizes a traffic encryption key (TEK) which is a string of hex characters of varying length depending on AES encryption protocol. Each TEK is assigned a Key ID (KID) and a Storage Location Number (SLN) that are used to select or index the desired TEK. Because modern subscriber units are capable of using several TEKs to encrypt transmissions, the SLN and KID are utilized so that the receiving equipment will know which encryption key to use to decode the transmission.

- **Constraints**

If a radio user or dispatch console utilizes encryption and other users on that talk group do not have the correct TEK, KID and SLN in their equipment, the user will not receive the message. Any radio voice logging equipment that does not have the appropriate TEK, KID and SLN will not log the voice traffic.

SLN/KIDs must be unique across the system.

While it is possible for more than one key to be identical, no two distinct encryption keys should use the same SLN/KID. E.g. if a region has SLN/KID "1" with a key of "00000000" and "0000000A"), this would cause the receiving unit (radio/console or voice logging equipment), to not accept one of the keys, or the unit would not know which key is appropriate for receiving an encrypted transmission with "SLN/KID 1".

3. Operational Context

The terminology "ISICS TEK(s)" references TEK(s) that are used for encrypted interoperability talk groups on the ISICS Platform.

4. Recommended Protocol/ Standard

ISICS TEKs and associated KIDs and SLNs used on the ISICS Platform must be kept secure.

No ISICS TEKs will be loaded or stored in any device where the key can be viewed. No ISICS TEKs will be stored in "plain text" in any device. It is also highly recommended that regional and locally owned and used TEKs not be allowed to be loaded or stored in a radio system device that stores the encryption keys in plain text.

No regional, local, or privately owned TEK may be loaded into any radio or console position without the approval of the owning Sub-System Administrator.

ISICS TEKs should only be distributed by the System Administrator, by using the following procedure to verify the identity of the sub-system administrator.

5. Recommended Procedure

The System Administrator or designee shall generate ISICS TEKs as necessary for their use. ISICS TEK(s) generated will be within the SLN/KID range designated and assigned by the System Administrator. The System Administrator(s) will be responsible for distributing the ISICS TEKs appropriately. ISICS TEKs used on the ISICS Platform must be kept secure. Subscriber radios, consoles, and logging solutions may require the use of a key loader/key fill device (KFD). The KFD is a device where the System Administrator or sub-system administrator enters the ISICS TEK(s) and associated SLN(s)/KID(s), and the key loader is then used to program the end user devices. KFDs used in conjunction with ISICS Platform must store the ISICS TEKs in an encrypted fashion and shall not display the individual key data.

The System Administrator shall only release an ISICS TEK to established sub-system administrators or designated personnel. Upon a request for an ISICS TEK, the System Administrator must look up the sub-system administrator in their files and call him/her at the phone number of place of employment. When satisfied that the correct sub-system administrator is reached, the System Administrator may verbally release the data. The ISICS TEK will not be emailed or transmitted electronically via plain text. The sub-system administrator shall then

store the written key in a secure location (e.g. locked safe with access to only the sub-system administrator or authorized designee) and destroy it once it has been added to a KFD. Any KFD should use an appropriate password to unlock the device for use.

The System Administrator will document the following for statewide TEKs:

- Which TEKs are allowed to be shared;
- Who the TEKs are shared with;
- When the TEKs were shared.

In special circumstances and with approval of the System Administrator, sub-system administrators can share ISICS TEKs with other sub-system administrators. The System Administrator will be notified so they may document the sharing of ISICS TEKs.

The TEKs should also be transferred from KFD to KFD or KMF to KMF, when technologically proven and practical, to minimize the chance for errors and to keep written copies of the keys to a minimum.

6. Management

Generation and storage of ISICS TEKs are the responsibility of the System Administrator or designee. Generation, storage and management of any local TEKs are the responsibility of the appropriate sub-system administrator.

The System Administrator is responsible for the correct programming of ISICS TEKs in all KFDs, KMFs. The sub-system administrators are responsible for console and subscriber radio programming.